NCSC-2

NATIONAL POLICY ON RELEASE OF COMMUNICATIONS SECURITY INFORMATION TO U.S. CONTRACTORS AND OTHER U.S. NONGOVERNMENTAL SOURCES

NATIONAL COMMUNICATIONS SECURITY COMMITTEE

NCSC

NATIONAL
COMMUNICATIONS
SECURITY
COMMITTEE

FOREWORD

This policy supersedes USCSB 12—13, National Policy on Authorizing U.S. Contractors Access to Classified Federal Telecommunications or Communications Security Material, dated 31 October 1973.

This policy no longer requires all nongovernmental personnel to have clearances based on background investigations (BIs). Individuals must possess a final government-granted security clearance at a level commensurate with the classification level of the accessed information. However, the clearances of facility security officers, COMSEC custodians, and alternate custodians must be predicated on a favorable BI current within five years.

This policy continues to delegate to the Heads of Federal Departments and Agencies the authority to release COMSEC information or material if all requirements of this policy are met. Provisions have been made for obtaining exceptions to the criteria and limitations contained in the policy,

FOR THE EXECUTIVE AGENT FOR COMMUNICATIONS SECURITY:

DONALD C. LATHAM
Chairman

NATIONAL POLICY ON RELEASE OF COMMUNICATIONS SECURITY INFORMATION TO U.S. CONTRACTORS AND OTHER U.S. NONGOVERNMENTAL SOURCES

7 July 1983

Section I—Scope and Applicability

1. This policy governs (a) release of classified and unclassified communications security (COMSEC) information to U.S. individuals who are not part of the Federal Government of the United States, hereafter referred to as the Government; and (b) use of U.S. nongovernmental sources for the conduct of government communications security activities. Provision of COMSEC information to foreign governments and international organizations is covered by NCSC-6.

Section II—Policy

2. Government communications security operations will ordinarily be conducted by the Government. The Government may obtain required COMSEC goods and services from, and may provide COMSEC information and material to, U.S. nongovernmental sources within the limitations of this policy.

3. Security standards and procedures applicable to any COMSEC information released outside of the Government shall in all cases be consistent with established national COMSEC doctrine and the specific requirements of this policy. In particular:

a. Individuals granted access to Government communications security information, must be U.S. citizens. Such access shall be controlled on a strict need-to-know basis and shall be granted only in conformance with procedures established for the particular type of COMSEC information involved. Requests for release of COMSEC information to U.S. individuals who are not U.S. citizens shall be processed as an exception to this policy.

b. Contracting for design, development, modification, production, or developmental testing of cryptographic equipment shall require the specific approval of the Director, National Security Agency (NSA).

c. As a prior condition of release, COMSEC information provided to U.S. persons not part of the Government shall be subsequently controlled in such a manner as to prevent its further dissemination outside of the Government or the unauthorized transfer of technology contained therein.

d. Individuals requiring access to U.S. COMSEC information must comply with applicable cryptographic access policies.

4. Government COMSEC information may be released outside of the Government when the following criteria can, be met:

a. A valid need must exist for an individual or organization to:

(1) Install, maintain, or operate communications security equipment for the U.S. Government;

(2) Participate in the design, planning, production, training, installation, maintenance, operation, logistical support, integration, modification, testing, or study of COMSEC material or techniques: or

(3) Electrically communicate classified national security information in a cryptographically secure manner, or unclassified national security-related information by COMSEC protected means.

b. Individuals granted access to classified COMSEC information must hold a final Government security clearance for the level of classification involved. The clearances of facility security officers, COMSEC custodians, and alternate COMSEC custodians must be predicated on a favorable background investigation current within five years.

c. All individuals provided access to COMSEC information must be briefed at least annually regarding the unique nature of COMSEC information and their security responsibilities to properly safeguard and control it.

d. All individuals who maintain Government COMSEC equipment must receive formal NSA-approved training on such equipment

Section III—Responsibilities

5. The Heads of Federal departments and agencies are responsible for:

a. Ensuring the requirements stated in this policy are met when contracting for COMSEC services as defined in paragraph 4.a. or when otherwise releasing COMSEC information outside the Government.

b. Determining that such releases are in the best interests of the Government.

c. Maintaining records of all organizations and self-employed individuals provided access to Government COMSEC information.

d. Notifying NSA of contract awards or other releases of COMSEC information and material; information provided should include the name of the contractor, licensee, or individual, the subject matter of the contract or provision, and the nature of the COMSEC information released;[1]

e. Ensuring that the performance of their contractors or licensees meets established COMSEC standards and doctrine, including standards of security and quality;

f. Incorporating the criteria specified in paragraph 4. above, into all contracts and other appropriate documents whenever individuals who are not employees of the Government will provide services identified in paragraph 4. above.

[1] The CIA is exempt from this requirement to the extent described in paragraph F. of the National Communications Security Directive

6. The Director, National Security Agency, is additionally responsible for:

a. Maintaining for the National Communications Security Committee (NCSC) a consolidated record of COMSEC contract and release notices furnished by other departments or agencies, and providing summary data on an annual basis to the Executive Secretary for forwarding to Members and Observers.

b. Approving waivers from established physical security standards for the protection of COMSEC information and material.

c. Providing assistance, when requested, to Heads of other departments and agencies in determining whether or not to use U.S. nongovernmental individuals and organizations for COMSEC activities and in administering requirements of this policy.

Section IV— Exceptions

7. Exceptions to this policy may be granted only by the NCSC, except for cases of waivers to physical security standards specified in paragraph 6.b. above which may be granted by the Director, National Security Agency. Prior approval must be obtained in each case, Requests for NCSC approval of an exception, with justification and explanatory details, shall be forwarded to the NCSC through the Director, National Security Agency, who shall provide appropriate recommendations for NCSC consideration. The checklist in the Appendix should be used as a guideline.

Section V—Definitions

U.S. Nongovernmenta/ Source. - An individual citizen of the United States or a U.S. corporation, association or other organization substantially composed of United States citizens, which is not directly a part of the Government (for example, a self-employed individual, consulting firm, licensee, or contractor, excluding active or reserve military personnel, Civil Service employees, and other individuals employed directly by the Government); specifically excluded are corporations or associations under foreign ownership, control, and influence.

COMSEC Information. - All information concerning COMSEC and all COMSEC material.

APPENDIX

CHECKLIST FOR PREPARING REQUESTS FOR EXCEPTIONS TO NCSC-2

1. Identify the individual and/or organization, their citizenship, their level of security clearance, and the location(s) at which COMSEC functions will be performed.

2. Identify the COMSEC functions the nongovernmental source(s} will perform, the COMSEC information and/or material to which the individual(s) will have access, the number of personnel involved, their training certification or any training required.

3. List the classification of the COMSEC information to which the source personnel will have access.

4. Indicate whether source personnel will be using keying materials marked "CRYPTO" which are held or used by Government departments and agencies. If so, has consideration been given to providing unique operational keying materials?

5. Indicate what additional administrative/security measures will be implemented.

6. Identify the inclusive dates for which source personnel will have access to COMSEC information under the provision of the contract or arrangement.

7. Identify the Government department or agency which will be responsible for assuring the security of nongovernment COMSEC operations/functions.

8. Identify the specific provision of NCSC-2 for which an exception is required.